

FILED

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

STEPHEN C. WILLIAMS
U.S. MAGISTRATE JUDGE
SOUTHERN DISTRICT OF ILLINOIS
EAST ST. LOUIS OFFICE

IN THE MATTER OF THE SEARCH OF)
)
A BLACK DROID MAXX, MODEL)
XT1080, CELLULAR TELEPHONE.)
)
A SILVER SAMSUNG TABLET,)
BEARING SERIAL NUMBER R22020PY6E.)

CASE NUMBER 14-mj-7088

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

a search warrant are as follows:

AFFIDAVIT

1. I am a SFO with the FBI assigned to the SCETF based in the FBI's Springfield Division, Fairview Heights, Illinois, Resident Agency. The SCETF is an FBI sponsored Task Force assembled to combat a variety of cyber-related crime in the Metro East area, and is comprised of law enforcement personnel from approximately fifteen (15) different local, state, and federal agencies. I have been assigned to the SCETF for approximately seven (7) years. My primary employment is as a sworn police officer for the Columbia Police Department, a position I have held for approximately 19 years. During this time, I have conducted and assisted in the investigation of state and federal offenses including the possession, receipt and transmission of images of child pornography and other sexual offenses against children. I have gained knowledge, experience, and training in such investigations through training seminars, classes, and work with other state and federal cyber-crime investigators. I have learned about the habits of child pornography collectors, distributors, and producers, those who exploit children online, and those who commit sexual offenses against children. I have been trained in the search and recovery of computers and peripherals, in the extraction of computer data and data from cellular telephones, and in the forensic preview of computers located at a suspect's residence. I have had the opportunity to observe and review numerous examples of child pornography, as defined in 18 U.S.C. §2256(8)(A), in all forms of media including computer media.

2. I make this affidavit in support of a warrant to search a **Black Droid Maxx, Model XT1080, Cellular Telephone, and a Silver Samsung Tablet, bearing serial number R22020PY6E (hereinafter "SUBJECT MEDIA")** taken from the residence of Richard Lee

Doerr, III, 2333 Old State Route 3, East Carondelet, Illinois, 62240, which is located within the Southern District of Illinois.

3. This affidavit seeks to search for and to seize contraband, evidence or instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A, specifically evidence related to the transportation, distribution, receipt and/or possession of child pornography from the **SUBJECT MEDIA**.

4. The statements contained in this affidavit are either based upon my investigation, information provided by other investigators, other personnel specially trained in the seizure and analysis of computers and electronic media, and on my experience and training as a Detective Lieutenant with the Madison County Sheriff's Office and an SFO with the FBI, as well as information provided by the Missouri Internet Crimes Against Children Task Force and United States Probation Officers. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Sections 2252 and 2252A exists on the **SUBJECT MEDIA**.

Searches of Electronic Media in General

1. It is my belief that the items sought in this affidavit for search warrant are stored electronically. Based upon my knowledge, training, and experience, I know that electronic files can be easily moved from a computer, cellular telephone, or other electronic storage medium to another. Therefore, electronic files downloaded to or created on a computer, cellular telephone, and/or other types of electronic media can be copied on or transferred to any other computer,

cellular telephone, other types of electronic media and/or storage medium at the same location. In addition, I know that searching computerized information for evidence of crimes often requires officers to seize most or all of a computer system(s) central processing unit and/or laptop computer(s), input/output peripheral devices, related software, documentation, storage media, and data security devices, including passwords, so that a qualified computer expert can accurately retrieve the system(s) data in a laboratory or other controlled environment. This is true because of the following:

a. Technical requirements: Searching computer systems, cellular telephones and/or other types of electronic media for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert and examiner is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since evidence from computer systems, cellular telephones and/or other types of electronic media is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code embedded in the system such as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

b. The analysis of electronically stored data, whether performed on-site or in a laboratory or other controlled environment, may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file "directories" and the

individual files they contain (analogous to looking at the outside of a file cabinet for the pertinent files, in order to locate the evidence and instrumentalities authorized for seizure by the warrant); “opening” or reading the first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; or performing electronic “keyword” searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

c. In some instances, the computer, cellular telephones and/or other types of electronic media “writes” to storage media without the specific knowledge or permission of the user. Generally, data or files that have been received via the Internet are automatically downloaded into a temporary internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to such data or files, and the files are only overwritten as they are replaced with more recently viewed internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer usage. Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a “picture” of what the computer system, cellular telephone and/or other type of electronic media was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer systems, cellular telephones and/or other types of electronic media’s operation, this information cannot be easily segregated.

d. Digital data on the hard drive that is not currently associated with any file,

may reveal evidence of a file that was once on the hard drive but has since been deleted or edited, or it could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and times the computer, cellular telephone and/or other type of electronic media was in use. File systems in computer systems, cellular telephones and/or other types of electronic media can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations.

e. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be learned from the absence of particular data on a digital device. Specifically, the lack of computer security software, virus protection, malicious software, evidence of remote control by another computer system, or other programs or software may assist in identifying the user indirectly and may provide evidence excluding other causes for the presence or absence of items sought by this application. Additionally, since computer drives may store artifacts from the installation of software that are no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timeliness of usage, confirming the identification of certain users, establishing a point of reference for usage, and, in some cases, assisting in the identification of certain users. This data can be evidence of a crime,

indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

2. Electronic files that have been “deleted” can be recovered months or years later using readily available forensic tools. When a person deletes a file on a computer, cellular telephone and/or other type of electronic media, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a computer, cellular telephone and/or other type of electronic media’s operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

Child Pornography Collector Characteristics

1. Based on my previous investigative experience related to child pornography investigations, the training I received on child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions on this subject, I

know there are certain characteristics common to individuals who collect, receive, distribute or transport images of child pornography:

a. Individuals who collect, receive, distribute, transport and/or possess child pornography have hoarding characteristics -- that is, these individuals collect and maintain their images and/or videos for long periods of time because of the great personal value the images have for the sexual gratification of the collector, the difficulty in obtaining the images as a result of their illegality, and their value to collectors because the images may be traded for new images with other collectors. This hoarding behavior likewise results in collectors transferring these images and/or videos to various forms of computer media, including, but not limited to, external hard drives, thumb drives, CDs and DVDs, rather than maintaining their collection in one central location for fear of loss of their collection and/or detection of their collection by law enforcement. This hoarding behavior among collectors of child pornography has been well established.

b. Individuals who collect, receive, distribute, transport and/or possess child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

c. Individuals who collect, receive, distribute, transport and/or possess child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, videotapes, books, drawings, or other visual media, such as anim . Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Furthermore, these individuals will often

also possess child erotica to lower the inhibitions of children they are attempting to seduce before using images and/or videos of child pornography to arouse the selected child partner or to demonstrate the desired sexual acts.

d. Individuals who collect, receive, distribute, transport and/or possess child pornography almost always possess and maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

e. Likewise, individuals who collect, receive, distribute, transport and/or possess child pornography often maintain their collections in digital or electronic format in a safe, secure and private environment, such as a computer and/or any other electronic media that may be found in the surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector’s residence, to enable the individual to easily view the collection, which is highly valued.

f. Individuals who collect, receive, distribute, transport and/or possess child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Individuals who collect, receive, distribute, transport and/or possess child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

Background of Investigation

1. On December 27, 2013, Tumblr, Inc., notified the National Center for Missing and Exploited Children (NCMEC) that thirty-four (34) possible images of child pornography had been uploaded to the “Tumblr.com” network by a computer with IP address 70.195.64.46. Tumblr identified the images as suspected child pornography by their hash values and subsequently shut down the account. Tumblr informed NCMEC that the person who uploaded the suspected child pornography used IP address 70.195.64.46, and that the individual had the following URL address: “http://loveteenspuss.tumblr.com,” user name “loveteenspuss” and email address “buddy_lee34@hotmail.com” associated with the account.

2. On January 16, 2014, NCMEC forwarded the cyber-tip to the Illinois Attorney General’s Crimes Against Children Task Force (ICAC), who subsequently forwarded it to the FBI’s SCETF, where the case was subsequently assigned to me. The information came in the form of password protected e-mail that contained the thirty-four (34) image files uploaded by “http://loveteenspuss.tumblr.com.” On May 27, 2014, I obtained a federal search warrant to view the thirty-four (34) image files that had been uploaded to the Tumblr.com network by Doerr. When I executed the search warrant, I found that, based on my training and experience, seventeen (17) of the images were of minors engaged in sexually explicit conduct, some of whom were prepubescent.

3. An open source search on Facebook for the e-mail address, "buddy_lee34@hotmail.com" led to "https://www.facebook.com/lee.doerr31," which was registered to Lee Doerr from Dupu, Illinois. On April 21, 2014, a subpoena was sent to Microsoft Online Services requesting subscriber information for "buddy_lee34@hotmail.com." The subpoena return indicated that the email address belonged to Lee Doerr from Illinois, 62239.

4. A search of the name Lee Doerr in the Consolidated Lead Evaluation and Reporting site, otherwise known as Clear, noted a Richard L. Doerr, II, with a date of birth in 1962, who lived at 2135 Mullins Creek Road, in Dupu, Illinois. The report also indicated that Richard L. Doerr, III, with a date of birth in 1987, also lived at this address. Finally, the report also provided the phone number of 618-830-0246 in connection with the Doerrs. A check of this telephone number revealed that it is registered to Richard L. Doerr, II, date of birth 1962, and has been active since July, 2004.

5. A subpoena was also sent to Verizon Wireless requesting, inter alia, the subscriber name, billing address and session times for the IP address (70.195.64.46) used when the images of child pornography were uploaded to "Tumblr.com" network on December 27, 2013. Verizon's response to the subpoena indicated that IP address 70.195.64.46 is a Nating Router IP, which are used by phone companies to provide internet access to multiple phone lines at the same time. Verizon attached a report containing all of the phone numbers that utilized that particular Nating Router IP during the time the images of child pornography were uploaded to "Tumblr.com," and I noted that the phone number associated with the Doerrs, 618-830-0246, was one of the telephone numbers used during that time frame.

6. When another open source search was conducted of Lee Doerr's Facebook account, I noticed that the profile pictures posted on the Facebook account matched the driver's license

picture of Richard L. Doerr, III, with a date of birth of 1987, the youngest Doerr (hereinafter "DOERR"). Conducting several open source searches, I also noted that this Facebook account was used almost daily, with the last time being October 2, 2014, the day I and several other FBI Special Agents and Special Federal Officers conducted a "knock and talk" at Doerr's residence.

7. On October 2, 2014, I and other FBI agents and SFOs went to 2135 Mullins Creek Road, Dupu, Illinois, to conduct a "knock and talk." When we arrived, we met with DOERR's father who told us that DOERR had not lived with him for approximately two years, but that DOERR still receives bills there. DOERR's father said that DOERR's current cellular phone number was 618-830-0246, but that it was his (the father's) name. He tried to call DOERR but there was no answer. DOERR's father gave us directions to DOERR's residence.

8. We went to DOERR's residence located at 2333 Old State Route 3, Apartment B, East Carondelet, Illinois, 62240, within the Southern District of Illinois. DOERR gave consent for us to enter his residence, and also agreed to provide a voluntary statement. When asked about his Tumblr account, DOERR admitted being the sole user of two Tumblr accounts, "loveteenspuss" and "Leezy87," as well as admitting that he shared child pornography images on both accounts. DOERR said that, around December 2013, he began using the "loveteenspuss" account to share child pornography but was blocked by Tumblr and the account was shut down. DOERR said that, around May 2014, he created another Tumblr account named "Leezy87," and shared some child pornography photos using this account, but that again blocked by Tumblr and the account was shut down.


9. DOERR said that he created a Kik Messenger account, using the user name "Leezy87," and that he shared child pornography pictures with other users using this account.

DOERR said that, when he received child pornography, he saved them to the Google Drive associated with his e-mail account, "leedoerr87@gmail.com." DOERR then provided us the account name and password for the Google Drive associated with his email account. DOERR also signed a Consent to Assume Online Presence Form allowing law enforcement agents to take over control of the e-mail account, "lee doerr87@gmail.com," and the Google Drive associated with the e-mail account.

10. While at DOERR's residence, DOERR consented to the search and subsequent seizure of the **SUBJECT MEDIA**, stating that he mainly used the Droid Maxx cellular phone to access the Internet and share images of child pornography. After DOERR willingly signed a Consent to Search form for the Droid Maxx cellular phone, FBI Special Analyst Velazco searched the cellular phone and found the both applications "Kik Messenger" and "Google Drive" had been installed on the cellular phone. When Special Analyst Velazco opened the Google Drive on DOERR's cellular phone, he saw more than fifty (50) images which, based on my training and experience, were of minors engaged in sexually explicit conduct, many of which were prepubescent. During the interview, DOERR later admitted using the Silver Samsung Tablet, which was synced to his Droid Maxx cellular phone, to share images of child pornography as well.

11. Based on the above information, your affiant believes there is probable cause to believe that the attached listed items, which are property constituting evidence of violations of Title 18, United States Code, Sections 2252 and 2252A, or property designed or intended for use or which is or has been used as the means of committing those criminal offenses which makes it a federal crime for any person to knowingly transport, distribute, receive and/or possess child pornography, will be found on the **SUBJECT MEDIA**.

FURTHER AFFIANT SAYETH NAUGHT.

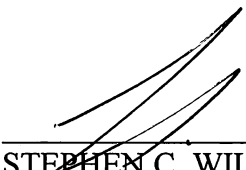

Karla F. Heine, Special Federal Officer
Federal Bureau of Investigation

STEPHEN R. WIGGINTON
United States Attorney

ANGELA SCOTT
Assistant United States Attorney

State of Illinois)
) SS
County of St. Clair)

Sworn to before me, and subscribed in my presence on the 28TH day of October, 2014, at
East St. Louis, Illinois.


STEPHEN C. WILLIAMS
United States Magistrate Judge

ATTACHMENT A

1. Any and all records and materials, in any format and media, pertaining to the possession, receipt, transportation or distribution of child pornography, as defined in Title 18, United States Code, Section 2256(8)(A).
2. All originals and copies of child pornography, as defined in Title 18, United States Code, Section 2256(8)(A), or child erotica, in any format and media.
3. Any and all records and materials, in any format and media (including, but not limited to, e-mail, chat logs and electronic messages) identifying persons transmitting through interstate or foreign commerce, including via computer, any child pornography, as defined in Title 18, United States Code, Section 2256(8)(A), or child erotica.
4. Any and all records and materials, in any format and media (including, but not limited to, envelopes, letters, papers, e-mail, chat logs, electronic messages, other digital data files and web cache information), bearing on the possession, receipt, transportation or distribution of child pornography, as defined in Title 18, United States Code, Section 2256(8)(A).
5. Records of communication (as might be found, for example, in digital data files) between individuals concerning the topic of child pornography, as defined in Title 18, United States Code, Section 2256(8)(A), the existence of sites on the Internet that contain child pornography or who cater to those with an interest in child pornography, as well as evidence of membership in online clubs, groups, services, or other Internet sites that provide or make accessible child pornography to its members and constituents.
6. Evidence of association, by use, subscription or free membership, with online clubs, groups, services or other Internet sites that provide or otherwise make accessible child pornography, as defined in Title 18, United States Code, Section 2256(8)(A).
7. Evidence of any online storage, e-mail or other remote computer storage subscription to include unique software of such subscription, user logs or archived data that show connection to such service, and user login and passwords for such service.
8. Digital camera software, graphics software, internet history files, movie files, user created directory and file names, electronic address books, correspondence, communications, internet and communication setting files, internet browser bookmark files, configuration files and password files.
9. Data files pertaining to the use of peer to peer file sharing software.
10. Data files indicating dominion, use and control of the computer, cellular telephone, electronic media, and/or physical or electronic storage device that contains them.